

Research on Security Applications Based on Cloud Computing Environments

Zhenhao Zhou

Wenzhou-Kean University, Wenzhou, Zhejiang, 325000, China

Abstract

With the rapid advancement of information technology, cloud computing has become a core component of modern information infrastructure, deeply integrated into daily life and various business scenarios. However, security risks related to confidentiality, integrity, and availability continue to pose persistent threats to cloud computing environments. This paper explores the foundational theories and security architectures of cloud computing, analyzes the challenges and key technologies in the field of cloud security, and proposes best practice-based security solutions tailored to the enterprise, government, and education sectors. The aim of this research is to provide a comprehensive understanding and guidance for the development of more secure and reliable cloud computing environments, offering valuable insights for further research and practical applications in related fields.

Keywords

cloud computing; architecture; cloud computing security; data security

基于云计算环境的安全运用研究

周桢豪

温州肯恩大学, 中国 · 浙江 温州 325000

摘要

随着信息技术的高速发展, 云计算已成为现代信息基础设施的核心组成部分并深度融入日常生活和各类业务场景, 然而机密性、完整性和可用性等方面的安全隐患仍然对云计算环境构成持续威胁。论文探讨了云计算基础理论和安全架构, 分析其在安全领域面临的问题和关键技术, 并针对企业、政府和教育领域提出了基于最佳实践的安全解决方案。论文的研究旨在为今后构建更安全、可靠的云计算环境提供较为全面的理解和指导, 并为相关领域的进一步研究与实践提供借鉴。

关键词

云计算; 架构; 云计算安全; 数据安全

1 引言

在工业革命 4.0 时代, 云计算作为信息技术的一次革命性飞跃, 已经被广泛应用于金融、医疗、教育、政府、制造业等领域。国内外各大厂家争相进入这个赛道, 国际有亚马逊 (AWS)、微软 (Azure) 和谷歌 (GCP) 三大领导者, 国内则有阿里云、腾讯云和华为云等各老牌厂商。通过基于互联网的集中资源模式, 云计算为个人和企业提供了弹性、高效和灵活的资源获取模式和计算能力, 然而其开放和共享的本质以及各大领域转型上云的加速使得云上安全问题日益显著, 尤其在基础设施安全、数据安全、身份和访问管理以及数据监控安全等方面成为不可忽视的挑战。

云上安全技术不仅要保证数据的机密性、完整性和可

用性, 还要为云计算服务的稳定、可靠运行提供坚实的基础。如何构建更加安全、可靠、稳定、易用的云计算环境成为当今时代的热点也是难点。论文从云计算基础架构的角度出发, 系统分析了当前云计算环境的主要安全隐患, 探讨了多层次安全架构设计的关键技术, 并针对企业、政府和教育领域提出基于最佳实践的安全解决方案, 旨在为云计算安全提供一定的指导意见。

2 云计算基础

2.1 基本概念和理论

云计算理论基础和特征是构建现代信息技术基础设施的核心。云计算的核心思想是将计算资源作为一种服务进行交付, 允许用户可以根据需求随时获取和释放大量资源, 从而实现高效、灵活和经济的计算能力, 其架构通常由基础设施即服务层 (IaaS)、平台即服务层 (PaaS) 和软件即服务 (SaaS) 层, 以及最近兴起的数据即服务层 (Data as a Software) 组成。

【作者简介】周桢豪 (1990-), 男, 硕士, 高级工程师, 从事通信工程、计算机网络、云计算、信息系统项目管理等研究。

在云计算的发展过程中,虚拟化技术(Virtualization)发挥着关键作用,通过软件定义资源的方式创建虚拟计算资源,使其能够被灵活地调度和分配,显著提高资源利用率的同时又实现资源的隔离;分布式计算则通过将计算任务分散到多个计算节点上,协同完成任务,提高计算能力和可靠性;存储技术包括分布式存储、对象存储和块存储,其中分布式存储和 NoSQL 数据库等技术则支撑起海量数据的存储和管理需求^[1];自动化工具(如 Ansible、Puppet、Chef)和编排技术(如 Kubernetes)能够自动化管理云环境中的资源和应用部署,提升效率,降低人为错误等;云计算安全技术则涵盖了数据加密、身份认证、访问控制、网络安全和合规性等方面。

2.2 核心特征

云计算的核心特征体现在其超大规模、抽象化、高可靠性、通用性、高可扩展性、按需服务、低成本、自动化和节能环保等方面。

超大规模的特征使得云计算能够支持数以万计的用户并发访问,抽象化则隐藏了底层复杂的技术细节,使得用户能够专注于应用的开发和使用;高可靠性通过冗余设计和故障恢复机制确保了服务的连续性;按需服务和高可扩展性使得用户可以根据需要动态调整资源,降低了运营成本;自动化和节能环保技术则进一步优化了资源的使用效率和环境的可持续性。

3 云计算安全架构

3.1 概念框架

云计算安全的概念框架是为了确保云计算环境中的数据和资源得到全面保护而产生的综合性保护模型。它覆盖了数据从创建到销毁的整个生命周期,包括数据的存储、使用、共享、归档和销毁等各个阶段^[2]。

云服务商是第一个关键部分,要满足在符合相关法律法规的情况下采用特定的指导方针和控制措施来确保用户数据的安全和隐私得到妥善保护。云计算安全服务体系构成了云计算安全概念框架的第二个关键部分,也叫责任共担模型,由用户和云服务商共同承担云上安全的责任。它由云基础设施安全服务、云安全基础服务和云安全应用服务三个层次组成,这些服务为云用户提供了实现其安全目标的重要手段。

3.2 存在问题和基本原则

云计算的开放和共享本质带来各种安全挑战,构建正确的云计算安全基本原则是保证云环境安全的基石,其为保护云中的数据、服务和基础设施提供了一套全面的指导方针。

①网络和基础设施的安全是云计算安全的第一核心原则。不合理的网络配置和搭配可能会导致网络在“南北向”都存在风险:如虚拟机间的隔离不当可能导致安全问题(虚拟机逃逸攻击),网络也可能遭受外部攻击(如 DDOS);云服务商本体故障和错误的“服务”搭配也有可能

导致安全问题,如使用不正确的存储策略可能导致数据丢失等。

②确保数据完整性和机密性,即数据在静态状态下和传输过程中的安全成为了关键性原则,如云上数据在多租户环境下的隔离不当或者内外部的恶意攻击都有可能

导致数据泄露或被篡改

③严格控制身份验证和访问控制是保障云计算安全的基础原则之一。随着远程工作的普及,对企业系统安全的远程访问设置不足和缺乏安全检查成为了突出问题^[3],错误的配置或弱密码都有可能

导致未经授权的恶意访问。

④合适的监控和日志手段是云计算安全的基础原则之一,缺少实时监控和日志管理往往会为后续故障和问题排查埋下隐患,实时监控云环境对监测和响应潜在威胁至关重要。

⑤数据可用性,即保证云服务的可用性和连续性的原则对于防止业务中断担任起最后保障的作用。系统故障、业务 bug、病毒,以及内外部的攻击等都有可能

3.3 关键技术

3.3.1 VPC 隔离及安全组管理

虚拟私有云(VPC)隔离和安全组(Security Group)管理是确保云环境网络安全的基础。VPC 提供逻辑隔离,使用户能够在云中创建独立的网络环境;安全组作为虚拟防火墙,控制进出 VPC 的流量,通过定义规则确保网络通信的安全性。

3.3.2 加密

加密技术是保护数据安全的重要手段,它通过将数据转换成不易解读的形式来防止未授权访问和泄露。在静态数据保护方面,云服务提供商通常使用对称加密算法(如 AES)和非对称加密算法(如 RSA 和 ECC)来确保存储在云中的数据的安全。在更高的安全等级要求下,也有使用“信封加密”对私钥进行再一次加密,并将此“信封密钥”存储于本地或者云服务商提供的 KMS 中从而进一步提高加密安全性。对于动态数据,即数据传输过程中的保护,则依赖于 SSL/TLS 等协议来实现端到端的加密,保障数据在传输过程中的安全。

3.3.3 授权

授权技术主要涉及身份认证与访问控制,确保只有合法用户才能访问相应的资源。身份认证是确认用户身份的过程,通常需要用户凭证信息。访问控制则基于用户身份和策略来决定其对资源的访问权限。在云计算环境中,可以通过身份和访问管理(IAM)系统来实现细粒度的访问控制,例如阿里云的 RAM 用户和角色管理。OAuth2.0 是一种广泛使用的授权框架,它允许第三方应用获得对用户数据的有限访问权限,而无需用户分享他们的凭据^[4]。此外多因素认证(MFA)为身份验证增加了一层额外的安全保护。

3.3.4 备份与恢复

数据的持久性与可恢复性是衡量云服务可靠性的重要指标。备份策略需要考虑备份的频率、类型（全量或增量）以及备份数据的存储位置。灾难恢复计划则包括数据恢复的优先级、恢复时间目标（RTO）和恢复点目标（RPO）等关键参数。现代云计算备份解决方案的优势在于可以根据数据和业务的类型提供多样化的具性价比的恢复方案，如 Amazon S3 和阿里云的 OSS 等云存储服务提供高可用性和持久性的存储解决方案，并支持多区域复制和版本控制，进一步增强数据保护能力。

3.3.5 实时监控和日志

实时监控云上的安全操作和日志的定期审计可以有效判断信息安全问题。云服务商通常提供集成的监控工具和服务收集和分析系统、应用和安全事件日志和操作日志等来发现问题。此外，安全信息和事件管理（SIEM）系统可以将不同来源的日志和事件进行关联分析，提供全面的安全态势感知和响应能力。

4 云计算安全应用场景

在云计算的广泛应用中，行业间既存在共性需求，也有各自独特的安全需求，不同行业需量身定制实践方案以满足各行业的特定要求和风险应对策略。

4.1 企业安全防护

企业由于面向互联网，其特点是用户基数大，对象复杂，因此需要建立全面的自动防护机制来应对大量的新颖、突变的安全问题。

通过整合云上的海量日志和用户行为形成安全态势感知平台，并借助先进的分析模型、数据湖，在巨大算力加持下进行 AI 运算来有效预警和阻止潜在威胁。此外自动化的安全运营给企业安全运维带来极大便利，比如可以集成某些特定安全服务，如 AWS Security Hub 来自动汇总和分析来自不同服务的安全数据，提供统一的安全视图，并且通过自动化规则和脚本实现安全事件的自动响应和修复，从而大大减少了人为干预和错误。

4.2 政府与教育领域的云计算安全

政府和教育机构作为国家单位，大多数是对内且敏感业务，其对于数据安全和数据管理的要求相对较高。

云计算安全需要遵循一系列政策环境和法规要求，如《个人信息保护法》《民法典》《中华人民共和国数据安全法》和《网络安全法》等，其中《数安法》要求建立数据分类分级保护制度，形成数据资源目录，并开展常态化的数据安全监测预警通报。这要求对数据进行细致梳理，明确数据类型和安全等级，实现数据资产的自动发现和目录的生成。

同时在安全管理方面需要强化运维人员的规范管理，培养构建安全责任模型的意识并和运营商共同承担云上责任，并严格控制运维变更。根据《云计算服务安全评估办法》，需要对云计算服务进行安全评估，以提高采购使用的云计算

服务的安全可控水平。此外加强应急预案和容灾备份措施，确保在遭受攻击或发生故障能快速恢复服务，保障业务连续性。例如，上海市在《上海市政务云管理暂行办法》中明确了政务云的运行维护和安全保障要求，包括建立网络安全事件管理制度和开展应急演练。

教育机构中还要强调教学的连续性和可靠性。设计高可用性的云计算架构，部署负载均衡和自动扩展\收缩机制来确保教学资源的灵活调配，尤其是在高负载下的无缝自动扩展能保证教学的稳定进行；也可以利用内容分发（CDN）技术，将教学资源分布到全球各地的边缘节点，提升访问速度也可以提高可靠性，确保视频、课件等教学资源的快速、稳定加载，提升学习体验等。

5 结论与展望

本文的研究针对基于云计算的网络信息安全技术进行深入分析，明确了通过探讨云计算的理论和安全架构，能够有效识别云计算环境下的安全挑战和关键技术，并据此提出针对企业、政府和教育领域的最佳实践安全应用方案。

随着技术发展，云计算安全领域的技术和方法也在不断革新和演进并带来新的挑战和机遇：零信任安全架构正逐渐成为主流，它强调在网络内外部都不应默认信任任何设备和用户，而是要求对所有访问请求进行严格的身份验证和访问控制，这种安全模型有望进一步增强云计算环境的安全性；人工智能和机器学习技术应用前景广阔，通过对大量安全数据的分析和建模，可以实现更加智能化的安全监控和威胁检测以及时发现和应对潜在的安全风险；量子计算的兴起对现有的加密技术构成了潜在威胁，量子计算机能够在极短时间内破解传统加密算法（如 RSA 和 ECC），为应对这一挑战，需要开发量子抗性加密算法（如格密码学）和新型的安全协议以确保云计算环境在量子计算时代的安全性^[9]等。

综上所述，随着技术的进步、法规的日益完善，我们有理由相信通过行业内外共同的努力可以更好的推动构建更加安全、可靠的云计算环境，为未来数字经济的发展保驾护航。

参考文献

- [1] 陈雪.云计算安全风险与保护技术框架研究[J].科技与创新,2023(5):68-70.
- [2] 童林萍,严雄兵,张荻.云平台安全架构及防护机制研究[J].网络安全技术与应用,2022(8):1.
- [3] 左咏梅.基于云计算环境的大数据审计平台构建研究[J].中小企业管理与科技,2020(1):1.
- [4] 王勇,徐衍龙,刘强.云计算安全模型与架构研究[J].信息安全研究,2019,5(4):6.
- [5] 单强.浅谈计算机云计算安全服务的架构[J].电子元器件与信息技术,2022(7):6.